EXHIBIT 1

CSC

Notice of Service of Process

SBR / ALL
Transmittal Number: 19157705
Date Processed: 12/31/2018

Primary Contact: James Cook
Jumio Corporation
268 Lambert Avenue
Palo Alto, CA 94306

Electronic copy provided to: Kasey Nemelka

Entity:	Jumio Corporation Entity ID Number 3581821
Entity Served:	Jumio Corporation
Title of Action:	Alex Prelipceanu vs. Jumio Corporation
Document(s) Type:	Summons/Complaint
Nature of Action:	Class Action
Court/Agency:	Cook County Circuit Court, IL
Case/Reference No:	2018CH15883
Jurisdiction Served:	Delaware
Date Served on CSC:	12/28/2018
Answer or Appearance Due:	30 Days
Originally Served On:	CSC
How Served:	Personal Service
Sender Information:	David Gerbie 312-893-7002

Information contained on this transmittal form is for record keeping, notification and forwarding the attached document(s). It does not constitute a legal opinion. The recipient is responsible for interpreting the documents and taking appropriate action.

To avoid potential delay, please do not send your response to CSC

251 Little Falls Drive, Wilmington, Delaware 19808-1674 (888) 690-2882 | sop@cscglobal.com

12-Person Jury

Return Date: No return date scheduled
Hearing Date: 4/23/2019 10:00 AM - 10:00 AM
Courtroom Number: 2510
Location: District 1 Court
Cook County, IL

FILED
12/21/2018 4:32 PM
DOROTHY BROWN
CIRCUIT CLERK
COOK COUNTY, IL
2018CH15883

FILED DATE: 12/21/2018 4:32 PM 2018CH15883

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

ALEX PRELIPCEANU, individually and on behalf of similarly situated individuals, *Plaintiff*, v. JUMIO CORPORATION, a Delaware Corporation, *Defendant.*	)	No. 2018CH15883 Hon. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Alex Prelipceanu, both individually and on behalf of similarly situated individuals, brings this Class Action Complaint against Defendant Jumio Corporation ("Jumio"), to stop its capture, collection, use, and storage of individuals' biometric identifiers and/or biometric information in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (the "BIPA"), and to obtain redress for all persons injured by its conduct. Plaintiff alleges as follows based upon personal knowledge as to his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

INTRODUCTION

1. BIPA defines a "biometric identifier" as any personal feature that is unique to an individual, including fingerprints, palm scans and facial geometry. "Biometric information" is any information based on a biometric identifier, regardless of how it is converted or stored. 740 ILCS § 14/10. Collectively, biometric identifiers and biometric information are known as "biometrics."

2. This case is about a cloud-based identity verification technology company capturing, collecting, storing, and using Plaintiff's and other consumers' biometric identifiers

and/or biometric information without regard to BIPA and the concrete privacy rights and pecuniary interests that BIPA protects. Defendant collects consumers' biometric information in the form of facial geometry through software it provides to its clients that in turn requires consumers to undergo an identity and/or age verification process which relies on Defendant's software. Consumers who seek to purchase goods or services from Jumio's clients and undergo Jumio's identity verification are required to upload a driver's license, photo ID, or passport. Consumers are then required to upload a photo of themselves or otherwise undergo a scan of their facial geometry, often taken through a webcam. Defendant uses its NetVerify technology to extract the biometric facial geometry templates of these customers and compare it to their photo ID. This allows for both identity verification and age verification, so the customer can proceed to make purchases of both goods and services from the Defendant's clients' businesses.

3. Using its NetVerify ID & Age Verification System software, Defendant captures, stores and uses consumers' facial geometry and related biometric information without complying with BIPA's requirements.

4. In recognition of the concern over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that private entities, such as Defendant, may not obtain and/or possess an individual's biometrics unless they first:

(1) inform that person in writing that the biometrics will be collected or stored;

(2) inform that person in writing of the specific purpose and the length of term for which the biometrics are being collected, stored and used;

(3) receive a written release from the person for the collection of the biometrics; and

(4) publish a publicly available retention schedule and guidelines for permanently destroying biometrics.

740 ILCS 14/5.

5. For companies wishing to comply with BIPA, such compliance is straightforward, and the necessary disclosures and a written release can be easily achieved through a single, signed sheet of paper. BIPA's requirements bestow upon consumers a right to privacy in their biometrics and a right to make an informed decision when electing to provide or withhold his/her most sensitive information and on what terms.

6. BIPA's statutory scheme requires that private companies like Defendant make specific disclosures to consumers prior to collecting their biometrics, which allows consumers the opportunity to make an informed choice when private entities request their biometrics. So, unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, and use biometrics and creates a private right of action for lack of statutory compliance.

7. In this case, Defendant elected to implement an invasive biometric face scanning program that relied on the illegal collection of consumers' biometrics, thereby invading their substantive privacy rights under BIPA.

8. Defendant implemented this biometric face scanning regime collecting facial geometry of its client's customers without first obtaining consumers' informed written consent, as required by law, and all while disregarding the relevant Illinois BIPA and the privacy interests it seeks to protect.

9. Defendant's conduct is particularly unsettling considering the fact that this extremely sensitive biometric information is also associated with consumers' government-issued identification documents. Despite the sensitive nature of this biometric information, Defendant

wholly avoids any costs associated with implementing its biometric identity and age verification system in compliance with the law.

10. The Illinois Legislature has found that "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, even sensitive information like Social Security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to each individual and therefore, once compromised, such individual has no recourse, is at a heightened risk for identity theft in, and is likely to withdraw from biometric facilitated transactions." 740 ILCS 14/5. The risk is compounded when, like in this case, a person's biometric information is also associated with government issued or other photo identification and related information.

11. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in capturing, collecting, storing, using, and transmitting his biometrics, and those of thousands of consumers throughout the state of Illinois, without informed written consent, and without informing them through a publicly available written policy of how it was going to store and dispose of this irreplaceable information, in direct violation of the Illinois BIPA.

12. Defendant failed to obtain the necessary consent to handle Plaintiff's and other consumers' biometrics; failed to maintain a lawful biometric storage program which deletes biometric information in the proscribed period; failed to provide the required disclosures at the time of collection; and failed to provide a retention and destruction schedule.

13. To the extent Defendant is still retaining Plaintiff's biometrics, such retention is unlawful and an ongoing infringement of his right to privacy regarding his biometrics as afforded

by the BIPA. Plaintiff would not have provided his biometrics to Defendant had he known that Defendant would retain such information for an indefinite period without his consent.

14. On behalf of himself and the proposed Class defined below, Plaintiff seeks an injunction requiring Defendant comply with BIPA, as well as an award of statutory damages to the Class, together with costs and reasonable attorneys' fees.

PARTIES

15. Defendant Jumio Corporation is a Delaware corporation that conducts business, and is licensed by the Illinois Secretary of State to conduct business, throughout Illinois and in Cook County. Jumio transacts business throughout the state of Illinois and knowingly transacts with Illinois residents.

16. At all relevant times, Plaintiff has been a resident and citizen of the state of Illinois.

JURISDICTION AND VENUE

17. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendant is doing business within this state and because Plaintiff's claims arise out of Defendant's unlawful in-state actions.

18. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101, because Defendant is doing business in Cook County and thus resides there under § 2-102, and because the transaction out of which this cause of action arises occurred in Cook County.

FACTS SPECIFIC TO PLAINTIFF

19. Defendant develops cloud-based identity verification technologies to companies that sell age-restricted consumer products over the internet.

20. Defendant openly acknowledges that it uses "advanced technology including biometric facial recognition, machine learning, and verification experts[.]"[1]

21. Defendant, using its NetVerify "ID & Age Verification System," captured, collected, stored, and transferred the biometric facial geometry of Plaintiff and other Illinois residents and consumers in violation of the BIPA. NetVerify "ID & Age Verification System" provides consumers the ability to purchase age-restricted products from Defendant's clients after confirming their age and identity through the use of biometrics.

22. Plaintiff verified his age and identity through Defendant's NetVerify system while purchasing products on the internet from one of Defendant's clients.

23. Through this identity and age verification process, Defendant captured, collected, stored, used, and transferred Plaintiff's biometrics in violation of the BIPA.

24. Before Plaintiff's biometrics were initially captured and collected, Plaintiff was required to also give his cell phone number to verify his phone number. Then he was required to upload his driver's license. Subsequently, Defendant took a biometric scan of Plaintiff's face through a "face scan" taken through Plaintiff's mobile device camera. Defendant then allowed Plaintiff to have access to its client's eCommerce platform so that he could proceed with his purchase.

25. Prior to taking Plaintiff's biometrics, Defendant did not inform Plaintiff in writing that his biometrics were being collected, stored, used, or disseminated, nor did Defendant publish any policy specifically about the collection, retention, use, deletion, or dissemination of biometrics. Defendant did not seek, and Plaintiff never provided, any written consent relating to the collection, use, storage, or dissemination of his biometrics.

[1] https://www.jumio.com/trusted-identity/netverify/ (last visited December 21, 2018).

26. Prior to taking Plaintiff's biometrics, Defendant did not make publicly available any written policy as to a biometric retention schedule and guidelines for permanently destroying the collected biometrics.

27. To this day, Plaintiff is unaware of the status of his biometrics obtained by Defendant. Defendant had not informed Plaintiff whether it still retains his biometrics, and if it does, for how long it intends to retain such information without his consent.

28. Plaintiff has suffered pecuniary damages in the form of diminution in the unique identifying value of his biometrics, and other costs associated with identity protection and account monitoring.

29. Furthermore, Plaintiff's biometrics are economically valuable and such value will increase as the commercialization of biometrics continues to grow. Defendant's use of Plaintiff's biometrics does and will continue to confer a benefit on Defendant at the expense of Plaintiff's privacy rights.

30. At the time Plaintiff's biometrics were captured, Defendant did not have a publicly available policy informing consumers, including Plaintiff, of what happens to their biometrics after they are captured, and what would happen to their biometric information if Jumio were to close, or if Defendant were to be acquired, sold, or file for bankruptcy. Plaintiff faces additional risks if Defendant were to suffer a data breach and lose not only Plaintiff's biometrics but also his personal identification documents.

31. As a result of Defendant's conduct, Plaintiff experiences severe mental anguish, anxiety, and other physical and mental injury when he thinks about the status of his biometrics and who has, or could have, access to such private information; what would happen to his biometrics if Defendant went bankrupt or otherwise sold its assets; whether Defendant will ever delete his

biometric information; what would happen if Defendant were to experience a data breach, and how any such breach would result in irreparable harm to the security of his identity. This harm is even more acute because an individual or entity with access to Plaintiff's biometrics could potentially access his other financial accounts or health records which may currently, or at some time in the future, be secured through his biometrics.

32. By failing to comply with BIPA, Defendant has violated Plaintiff's substantive state rights to biometric information privacy.

CLASS ALLEGATIONS

33. Plaintiff brings this action on behalf of himself and a class of similarly situated individuals pursuant to 735 ILCS § 5/2-801. Plaintiff seeks to represent a Class as defined as follows:

> All individuals whose biometrics were captured, collected, stored, used, transmitted, or disseminated by Defendant Jumio within the state of Illinois any time within the applicable limitations period.

34. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant and any immediate family member of such officer or director.

35. Upon information and belief, there are thousands of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiff, the members can be easily identified through Defendant's records.

36. Plaintiff's claims are typical of the claims of the Class he seeks to represent, because the factual and legal bases of Defendant's liability to Plaintiff and the Class is the same, and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class. As

alleged herein, Plaintiff and the Class have all suffered damages as a result of Defendant's BIPA violations and various common law transgressions.

37. There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant made available to the public a written policy that establishes a retention schedule and guidelines for destroying biometrics;

b. Whether Defendant obtained a written release from the Class before capturing, collecting, or otherwise obtaining their biometrics;

c. Whether Defendant provided a written disclosure to the class that explains the specific purposes, and the length of time, for which their biometrics were being collected, stored and used before taking their biometrics;

d. Whether Defendant's conduct violates BIPA;

e. Whether Defendant's conduct is negligent;

f. Whether Defendant's conduct constitutes an invasion of privacy;

g. Whether Defendant's violations of the BIPA are willful or reckless; and

h. Whether Plaintiff and the Class are entitled to damages and injunctive relief.

38. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

39. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class.

40. Defendant has acted and failed to act on grounds generally applicable to the Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*, (On behalf of Plaintiff and the Class)

41. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

42. Defendant is a private entity under BIPA.

43. Plaintiff and the Class members had their biometric identifiers collected, captured, received or otherwise obtained and/or used by Defendant.

44. Defendant captured, collected, stored, and/or used Plaintiff's and the Class members' biometrics without valid consent and without complying with BIPA through its biometric identity and age authentication software.

45. Plaintiff and the Class members have been aggrieved by Defendant's failures to adhere to the following BIPA requirements, with each such failure constituting a separate and distinct violation of BIPA:

a. Defendant failed to inform Plaintiff and the Class members in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);

b. Defendant failed to inform Plaintiff and the Class members in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

c. Defendant failed to inform Plaintiff and the Class members in writing of the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

d. Defendant failed to obtain a written release from Plaintiff and the Class members, as required by 740 ILCS 14/15(b)(3);

e. Defendant failed to provide a publicly-available retention schedule detailing the length of time the biometrics are stored and/or guidelines for permanently destroying the biometrics it stores, as required by 740 ILCS 14/15(a); and

f. Defendant failed to obtain informed consent to disclose or disseminate the Class members' biometrics, as required by 740 ILCS 14/15(d)(1).

46. By capturing, collecting, storing, using, and disseminating Plaintiff's and the Class members' biometrics as described herein, Defendant denied Plaintiff and the Class members their right to statutorily-required information and violated their respective rights to biometric information privacy, as set forth in the BIPA.

47. Had Defendant informed Plaintiff that he was not being provided with the required information regarding his biometrics and the biometric face scanning program as required by law, he would not have provided his facial biometrics to Defendant.

48. Had Defendant informed Plaintiff that he would be asked to participate in an illegal biometric face scanning program, Plaintiff would not have used Defendant's biometric face scanning system, or he at least would have been able to make an informed decision concerning material facts of his use of the NetVerify "ID & Age Verification System," including whether the benefit justifies the increased risk in participating in Defendant's unlawful biometric program.

49. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of the BIPA.

50. Defendant's violations of BIPA, as set forth herein, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with the BIPA disclosure, consent, and policy posting requirements.

51. Accordingly, with respect to Count I, Plaintiff, on behalf of himself and the proposed Class, prays for the relief set forth below.

COUNT II
Negligence
(On behalf of Plaintiff and the Class)

52. Plaintiff hereby incorporates the foregoing allegations as if fully set forth herein.

53. To the extent that a finder of fact concludes that Defendant did not intentionally withhold information from Plaintiff and the Class relating to its biometric facial geometry scan program, Defendant was nonetheless careless and negligent in its failure to act reasonably with regards to its biometric program.

54. A special relationship existed between Plaintiff and the Class and Defendant which gave rise to various duties and obligations concerning the biometric face scans and biometric data at issue because Defendant had full control over such biometric program, policies, and procedures relative to Plaintiff's and the Class members' limited knowledge and power.

55. Indeed, Defendant's position relative to Plaintiff in terms of access to information regarding the technology at issue, and its conduct in handling Plaintiff's biometrics, gave rise to a duty for Defendant to act reasonably in the circumstances.

56. Defendant knew, or should have known, of the risks inherent in collecting, storing, using, and disseminating biometrics and owed duties of reasonable care to Plaintiff and the Class members whose biometrics were obtained by Defendant.

57. Defendant breached its duties to Plaintiff and the Class with regards to biometric privacy by, among other things, failing to implement a BIPA-compliant biometric system with reasonable data security policies.

58. As a direct and proximate result of Defendant's conduct in failing to act reasonably with regards to its biometric program, Plaintiff and the Class members have suffered a diminution in the value of their biometrics caused by Defendant's collection, use, and exposure of such information.

59. Accordingly, with respect to Count II, Plaintiff, on behalf of himself and the proposed Class, prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, respectfully requests that this Court enter an Order:

a. Certifying the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;

b. Declaring that Defendant's actions, as set forth herein, violate the BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with the BIPA

requirements for the capture, collection, storage, use, and dissemination of biometric identifiers and biometric information;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(1);

e. Awarding statutory damages of $1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(3);

f. Awarding monetary damages and/or equitable relief for Defendant's common law violations in an amount to be determined at trial;

g. Awarding reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);

h. Awarding pre- and post-judgment interest, as allowable by law; and

i. Awarding such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Dated: December 21, 2018

Respectfully Submitted,

ALEX PRELIPCEANU, individually and on behalf of a class of similarly situated individuals

By: /s/ David Gerbie
One of Plaintiff's Attorneys

Myles McGuire
David L. Gerbie
Jad Shekali
MCGUIRE LAW, P.C. (Firm ID: 56618)
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
(312) 893-7002
Fax: (312) 275-7895
mmcguire@mcgpc.com
dgerbie@mcgpc.com
jsheikali@mcgpc.com

Attorneys for Plaintiff and the Putative Class